情報システム基盤に関する基礎技術の修得

第三技術室システム設計技術班
水野広治，鈴木重寛，松山幸雄，吉田祥造

1. はじめに

現在，多くの企業・官公庁等でIPネットワークによるLANが構築されており，電子媒体による情報交換が当然のように行われている．電子メールやWeb掲示板などの身近なもの，電子会議やグループウェアなどのビジネス的な色合いを持つものなど，利用の形態は多種多様である．しかしながら，転送される情報はネットワーク上で絶えず漏洩等の危険を抱えており，何らかの保護手段を講じる必要がある．

今回の研修では，ネットワークの基本的な情報技術及びVPN（Virtual Private Network）を実現するPPTP (Point to Point Tunneling Protocol), IPsec (IP SECurity) 及びSSH (Secure SHell) のプロトコルを学んだ．更に実習では，LANケーブルの製作と学内ネットワーク上の離れた地点の異なるセグメント間でVPNを構築し，Windows 2000，Linux及びVPNルータでの相互通信を実験的に検証したので報告する．

2. VPNの概要

VPNとは，一般的に不特定多数が共有するインターネット等のネットワーク回線上に，仮想的な専用回線を構築する手法である．IPネットワークでは，送信データをパケットと呼ばれる単位に分割して送信する．パケットはパケットの種類，サイズ，発信元アドレス，送信先アドレスなどが記述された「ヘッダ」部と，通信データ本体の「ペイロード」部で構成される．端末から送信されたパケットは，ヘッダ情報をもとに，論理的に最短な伝送路を選択して送信され，送信先で再び元のまとまったデータに組み立てられる．パケットのペイロード部はネットワーク間の通信の制御には一切関知しない．これらの事を応用すれば，パケットの前に更に別のヘッダを付加する事で，元のパケット自体をペイロード部として包み込み新しいパケットが生成される．これを「パケットのカプセル化」と呼ぶ．VPNでは，このカプセル化を施した上で送信情報の認証・暗号化を行う．

認証・暗号化に関しては，既にS/MIME（Secure MIME）やSSL（Secure Sockets Layer）等のプロトコルでも実現されているが，これらのプロトコルはネットワーク相互の接続後に特定のアプリケーション上で機能する．これに対してVPNでの認証・暗号化はネットワーク相互の接続時点より行われるため，接続後に使用するアプリケーション全てにおいてデータの保護が可能となる．

VPNで使用するプロトコルとしては，PPTP，IPsec，L2TP（Layer 2 Tunneling Protocol）等があるが，研修では，IP規格のIPv6から考案されたIPsec上での検証を行っている． IPsecの機能は，Windows 2000，Windows XPやFreeBSDでは実装されているが，LinuxでIPsecを行う場

合はFreeS／WANというソフトウェアをインストールする必要がある．

3. 暗号と認証

ネットワークの通信において，何も加工しない平文データで通信すると，そのデータをパケットモニタなどのツールやプログラムで簡単に盗聴することができ，情報の漏洩などが発生する．そこで，VPNでのセキュリティ対策は，通信データの暗号化と認証の組み合わせにより行われる．暗号化の目的には，通信の盗聴を防止する「(通信の) 機密性の保証」，他のユーザやホストの“なりすまし”による「(送信者の) 正当性の検証」，通信データの“改ざん”による「(データの) 完全性の検証」の３つがある．

図3は，暗号技術の相関図を示したもので，各々の暗号技術の欠点を相互に補い合い，協力することにより暗号化を実現している．VPNの主要プロトコルであるIPsecは，実線で示しているとおりほとんどに関係している．以下主要なものについての説明を行う．

「機密性の保証」をするための通信データの暗号化の方式には，データの暗号化と復号化を同じ鍵(共通鍵)を用いる共通鍵暗号方式(DES,3DESなど)と，暗号化用鍵(秘密鍵)と復号化用鍵(公開鍵)を用いる公開鍵暗号方式(Diffie-Hellman,RSAなど)がある．公開鍵暗号方式の安全性は，秘密鍵の安全性と公開鍵の正当性と完全性により保証される．公開鍵は脅威にさらされるため，その正当性と安全性はPKI(Public Key Infrastructure：公開鍵基盤)によって保証される．尚，PKIは認証局に公開鍵を登録することにより，そこから発行される証明書によって公開鍵を保証している．共通鍵暗号方式の安全性は，共通鍵の安全性が前提で，お互い共有する共通鍵の安全性は，公開鍵暗号方式やDiffie-Hellmanによって行われるが，Diffie-Hellmanには共有する相手の正当性の検証を行う機能が存在しないため，電子署名により行なわれる．

「正当性や完全性の検証」の実現はMAC(Message Authentication Code：メッセージ認証コード)や電子署名によって行う．MACは，共通鍵の使用をもとにハッシュ関数(MD5,SHA-1など)を利用したHMAC(Hashed based MAC)または共通鍵暗号方式による方法によって生成され，共有された共通鍵を利用して検証される．電子署名は，ハッシュ関数と公開鍵暗号方式によって生成され，認証データと共に送ることによりデータの正当性や完全性の検証ができる．

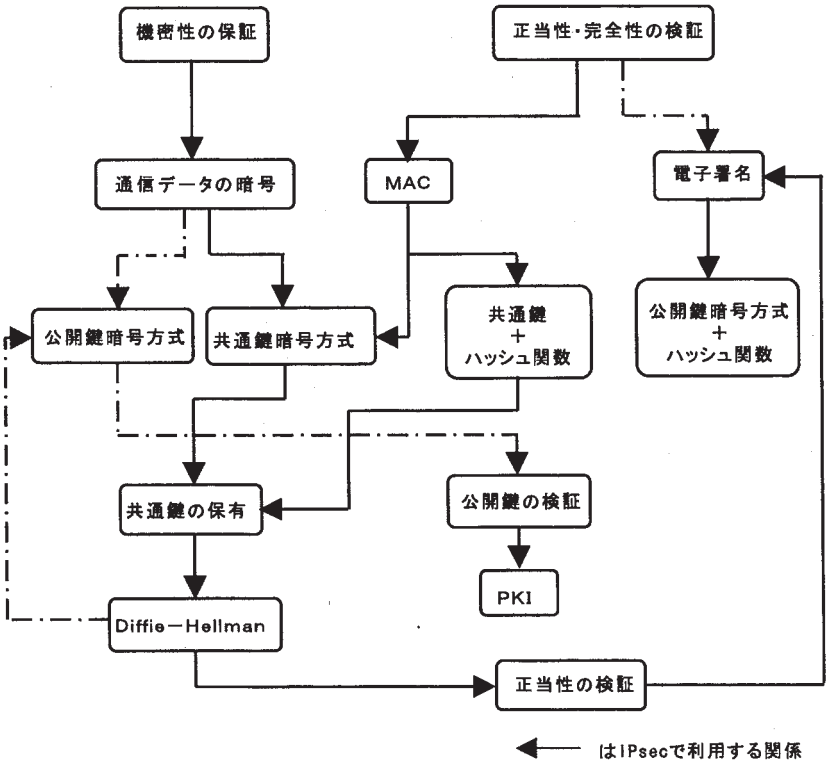

図3 暗号技術の相関図

4. IPsecとは

IPsecは，IPパケットをパケット単位で暗号化し認証するセキュリティプロトコルで，次期TCP／IPプロトコルのIPv6では標準で実装されている．IPsecは，大きく3つのプロトコルで構成されている．まず，AH（Authentication Header）プロトコルで通信データの認証を，ESP（Encapsulating Security Payload）プロトコルで通信データの暗号化を行う．IPsecではAHとESPを総称してセキュリティプロトコルとも呼ばれている．3つ目のIKE(Internet Key Exchage)プロトコルで通信相手の認証，AHやESPで用いる秘密鍵の交換を自動的に行う．IPsecの暗号化方式は，共通鍵暗号方式が採用されている．

ここでは，IPsec通信の全体像をつかむため一連の流れ（**図4**参照）を簡単に説明する．

第1のステップは，「どのようなパケットに，どのようなセキュリティサービスを，どのようなアルゴリズムを利用して提供するか」，「どのようなパケットにはセキュリティサービスを提供しないか」等，あらかじめSP（Security Policy）を作成してSPD（Security Poricy Database）に登録する．これにより，IPsec通信で提供するセキュリティサービスを決定する．

第2ステップは，IKEによりSA（Security Association）や秘密鍵の折衝を行う．SAの折衝とは，通信相手に複数の提案（パラメータセット）を含むIKEパケットを送信する．通信相手は，受信したIKEパケット内の複数の提案から一つを選択し，応答IKEパケットとして通信元に返信する．このようなやりとりを繰り返してSAが確立する．次に使用するDiffie-Hellman鍵交換アルゴリズムで秘密鍵を交換する．この秘密鍵で，認証データの暗号化と復号化が，HMACにより行われる．IKEには，HMACを使用することで通信相手の正当性とデータの完全性を検証する機能がある．

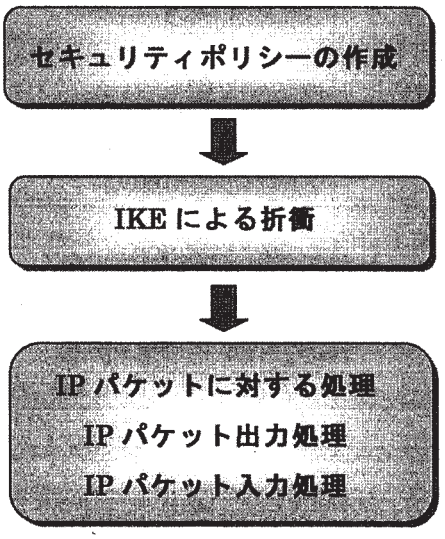

図4 IPsec通信の流れ

第3ステップは，検索されたSPやSAの内容から，IPパケットに使用するアルゴリズム，秘密鍵，暗号処理に必要な初期化ベクトルなどが決定する．IPパケットの出力処理は，セキュリティ処理を施す前に，必要に応じてIPComp（IP payload COMPression）による圧縮処理を行う．この圧縮はパケット単位の圧縮のため，圧縮後のデータの方が圧縮前に比べ大きくなることがある．この場合は，圧縮前のデータを送信する．その後，AHではAHヘッダの挿入や認証データの生成，ESPではESPヘッダの挿入や秘密鍵暗号を使用してデータを暗号化して下位層に受け渡す．この時点で，パケットのサイズがMTU(Maximum Transfer Unit)を超えている場合，フラグメント処理でパケットのサイズを小さく分割して送信する．一方，IPパケットの入力処理は，基本的に出力処理の逆の処理を行い，上位層への受け渡し，もしくは他のホストへのIPパケットの転送を行う．

IPsecのモードには，ホスト間のセキュリティを高める「トランスポートモード」と，ネットワーク経由での通信のセキュリティを高める「トンネルモード」がある．トランスポートモードは，IPパケットのペイロード部分のみを暗号化して送信する．一方トンネルモードは，他のホストからいったん受信したIPヘッダとペイロード部分を合わせたものをまとめて暗号化した上で，新たにIPヘッダを再度付け直して送信する．

5. 実験実習

5.1. LAN ケーブル作り

LAN ケーブルは，ネットワーク構築には必要不可欠なものである．そこで，研修者が実際に VPN 構築の実習で使用する UTP ケーブルを自作することにした．接続用途により配線が異なるストレートとクロスの 2 種類のケーブルを作製した．

5.2. IPsec による VPN の構築

IPsec による VPN の構築を，PC 又はルータ間で実現するために計 6 回の実習を行った．実習では，実際にいくつかの構成（**図 5.1**）にて，研修者全員が IPsec による VPN の構築を検証した．検証のための構成は，Windows 間（**図 5.1Ⓐ**），Windows と Linux 間（**図 5.1Ⓐ**），Windows 又は Linux と VPN ルータ間（**図 5.1Ⓑ**），それにＶＰＮルータ間（**図 5.1Ⓒ**）を主な組み合わせとした．また，各派遣先のネットワーク間相互での IPsec による通信の確認も行った．今回実習に使用した VPN ルータ（MR104DV）の機能を**リスト 5.1** に示す．

ネットワークインターフェース ： WAN×１(10/100)， LAN×４(10/100)，DMZ×１(10/100)
DHCP 機能 ： サーバ/クライアント
VPN 対応プロトコル ： IPsec（パススルー）， PPTP（パススルー），L2TP（パススルー）
IPsec 仕様 ： 暗号-DES, 3DES, ハッシュ-MD5, SHA-1 トンネル-50, 鍵交換-IKE（メイン/アグレッシブ）
ファイアウォール ： SPI, DoS, パケットフィルタリング
設定方法 ： WEB ブラウザ

リスト 5.1 研修で使用した VPN ルータの主な機能

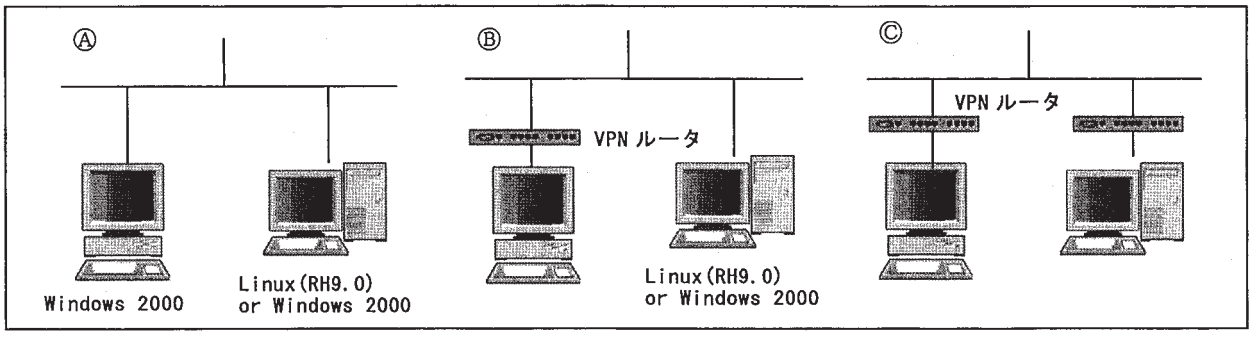

図 5.1 VPN(IPsec)構築の実習におけるマシンの組み合わせ

5.2.1. Windows 間での IPsec 構築

Windows 間（**図 5.1Ⓐ**）での VPN 構築は比較的容易である．システム自体に標準で IPsec が実装されており，ホスト間で IPsec 通信を行う処理内容を予め取り決めて（**リスト 5.2**），お互いの「ローカルセキュリティポリシー」にて設定（**リスト 5.3**）することで IPsec による通信のための準備が整う．更に，確認ツール「ipsecmon」（**図 5.2**）が用意されており，確立された SA

処理モード：トンネル／トランスモード
セキュリティプロトコル：ESP
暗号アルゴリズム：３DES
認証アルゴリズム：SHA-1
PFS：有効
接続先認証：事前共有鍵方式

リスト 5.2 IPsec 通信のための取り決め

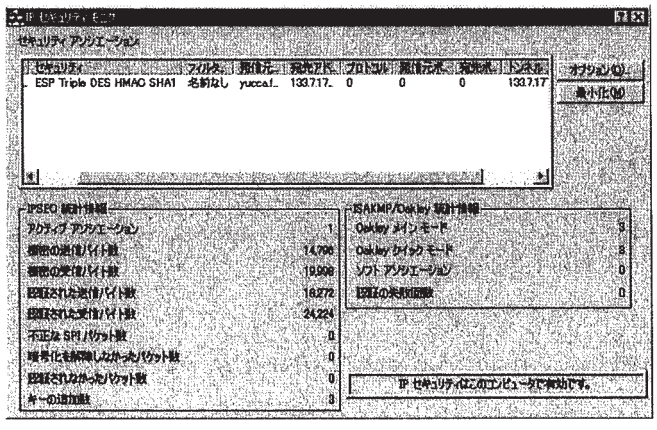

図 5.2「ipsecmon」による IPsec 確立の確認

1. 「ローカルセキュリティ設定」の起動
   「スタート」→「コントロールパネル」→「管理ツール」→「ローカルセキュリティポリシー」
2. 対象ホストやプロトコルの設定【発信先／元アドレスとプロトコルの種類を設定】
   「ローカルコンピュータのIPセキュリティポリシー」右クリック→「IPフィルター覧とフィルタ操作の管理」→
   「IPフィルター覧の管理」タブ「追加」→「IPフィルター覧」「追加」→「IPフィルタウィザード」
3. IPフィルタに対する操作の設定【パケットの処理方法や暗号アルゴリズムを設定】
   「IPフィルター覧とフィルタ操作の管理」→「フィルタ操作の管理」タブ「追加」→「フィルタ操作ウィザード」
4. IPセキュリティポリシーの作成
   「ローカルコンピュータのIPセキュリティポリシー」右クリック→「IPセキュリティポリシーの作成」→
   「IPセキュリティポリシーウィザード」→作成した「IPセキュリティポリシーのプロパティ」→「規則」タブ「追加」
5. いつ，どのように開始するかの指定【設定したIPフィルタ／フィルタ操作の指定と認証方法を設定】
   「セキュリティの規則ウィザード」→「IPセキュリティポリシーウィザード」→「セキュリティの規則ウィザード」
6. 鍵交換に関する設定【PFSとIKE SAの暗号／認証アルゴリズムなどを設定】
   「ローカルセキュリティポリシー」→作成した「IPセキュリティポリシーのプロパティ」→「全般」タブ「詳細」→
   「キー交換の設定」→「メソッド」→「キー交換のセキュリティメソッド」
7. 設定の有効化
   「ローカルセキュリティポリシー」→作成した「IPセキュリティポリシーのプロパティ」右クリック→「割り当て」

リスト5.3 Windows 2000によるIPsec通信のための基本的な設定の流れ

や通信の情報を知ることができる．

5.2.2. Windowsと Linux間でのIPsec構築

Windowsと RedHat 9.0(RH9.0)を用いてVPN構築を行った（**図5.1Ⓐ**）．Windows 2000の設定は，基本的には先述の設定と同じである．RH9.0では，IPsec実現のためにFreeS/WANパッケージ（**リスト5.4**）を入手しインストールを行った．設定は，**リスト5.2**の内容で設定ファイルipsec.confとipsec.secretsを編集する．具体的な設定内容と再起動処理を**リスト5.5**に示す．また，パケットキャプチャツール「tcpdump」によるpingのIPsec通信内容を**図5.3**に示す．

```
# cat /etc/ipsec.config
version 2.0
config setup
        interfaces=%defaultroute
        rp_filter=0
        klipsdebug=none
        plutodebug=none
        pluto=yes
        plutowait=no
        uniqueids=yes
conn  %default
        type=tunnel
        auth=esp
        authby=secret
        pfs=yes
        keylife=1h
        ikelifetime=8h
conn    IPsectest
        left=133.7.17[illegible]
        leftnexthop=%defaultroute
        right=133.7.4[illegible]
        auto=start
# cat /etc/ipsec.secrets
133.7.17[illegible] 133.7.4[illegible] : PSK "ipsectest-key"
# /etc/init.d/ipsec restart
ipsec_setup: Stopping FreeS/WAN IPsec...
ipsec_setup: Starting FreeS/WAN IPsec 2.04...
ipsec_setup: Using /lib/modules/2.4.20-8/kernel/net/ipsec/ipsec.o
```

（自身のIPアドレス：left=133.7.17[illegible]）
（相手のIPアドレス：right=133.7.4[illegible]）
（IPsecの再起動：# /etc/init.d/ipsec restart）

リスト5.5 FreeS/WANの設定ファイルと再起動

```
freeswan-module-2.04_2.4.20_8-0.i386.rpm
freeswan-userland-2.04_2.4.20_8-0.i386.rpm
```

リスト5.4 FreeS/WAN RPMパッケージ

```
# tcpdump -n host 133.7.4[illegible]                    通常のping通信
17:24:21.818801 IP 133.7.17[illegible] > 133.7.4[illegible]: icmp 64: echo request seq 1
17:24:22.829021 IP 133.7.17[illegible] > 133.7.4[illegible]: icmp 64: echo request seq 2
17:24:23.830565 IP 133.7.17[illegible] > 133.7.4[illegible]: icmp 64: echo request seq 3
17:27:01.702686 IP 133.7.4[illegible].500 > 133.7.17[illegible].500: [|isakmp]
17:27:01.706732 IP 133.7.17[illegible].500 > 133.7.4[illegible].500: [|isakmp]   IPsec
17:27:01.927523 IP 133.7.4[illegible].500 > 133.7.17[illegible].500: [|isakmp]   折衝中
17:27:01.967324 IP 133.7.17[illegible].500 > 133.7.4[illegible].500: [|isakmp]
17:27:02.041912 IP 133.7.4[illegible].500 > 133.7.17[illegible].500: [|isakmp]
17:27:02.044756 IP 133.7.17[illegible].500 > 133.7.4[illegible].500: [|isakmp]
17:27:02.266187 IP 133.7.4[illegible].500 > 133.7.17[illegible].500: [|isakmp]
17:27:02.306490 IP 133.7.17[illegible].500 > 133.7.4[illegible].500: [|isakmp]
17:27:02.382778 IP 133.7.4[illegible] > 133.7.17[illegible]: ESP(spi=0x4c86fcf0,seq=0x1)
17:27:02.383141 IP 133.7.4[illegible].500 > 133.7.17[illegible].500: [|isakmp]
17:27:02.649469 IP 133.7.17[illegible] > 133.7.4[illegible]: ESP(spi=0x65b8ef3a,seq=0x1)
17:27:02.650086 IP 133.7.4[illegible] > 133.7.17[illegible]: ESP(spi=0x4c86fcf0,seq=0x2)
17:27:03.659568 IP 133.7.17[illegible] > 133.7.4[illegible]: ESP(spi=0x65b8ef3a,seq=0x2)
17:27:03.660076 IP 133.7.4[illegible] > 133.7.17[illegible]: ESP(spi=0x4c86fcf0,seq=0x3)
                                                    IPsecによるping通信
```

図5.3 IPsec適用前後のパケットキャプチャ内容

5.2.3. Windows 又は Linux と VPN ルータ間での IPsec 構築

Windows や RH9.0 を対象に VPN ルータとの間で VPN の構築を行った(**図 5.1Ⓑ**). 設定により, VPN ルータの LAN 側サブネット（プライベート可）に接続の PC が VPN ルータ越えの通信を行う場合, VPN ルータと通信相手との間では, IPsec による通信となる. この時, LAN 側 PC の設定は必要がない. 尚, VPN ルータの設定は, Web ブラウザで設定する.

5.2.4. VPN ルータ間での IPsec 構築

VPN ルータ間での VPN 構築（**図 5.1©**）は, 今回, 同じルータ間での設定となるため構築は簡単であった. Web ブラウザによる設定後は, 各ルータの LAN 側に接続された PC 相互の通信が, ルータ間では IPsec による通信となる.

6. 研修日程

実施日時	研修内容
8月11日 13:30～15:00	専門研修の具体的な進め方を協議
10月15日 10:00～12:00	ネットワーク, 暗号の基礎知識, VPN 実現のプロトコル(輪講)
10月22日 10:00～12:00	LAN 間接続 VPN とリモート VPN, トンネリング, インターネット VPN(輪講)
10月29日 10:00～12:00	暗号技術の構成, ハッシュ関数, 共通鍵暗号方式と公開鍵暗号方式(輪講)
11月12日 10:00～12:00	ネットワーク接続ケーブル作製の実習（情報メディア研究室）
11月26日 10:00～12:00	電子署名と PKI, IPsec を構成する概念とプロトコル, セキュリティ(輪講)
12月 3日 10:00～12:00	IPsec 通信の概要, セキュリティポリシー, IKE, IP パケット(輪講)
12月10日 10:00～12:00	IPsec 通信における AH(ESP)パケットの構造, AH(ESP)の処理フロー(輪講)
12月17日 10:00～12:00	IPsec における IKE の機能, IKE パケットの構造, IKE の処理フロー(輪講)
12月22日 10:00～12:00	VPN ルータの機能と各種設定の実習（情報メディア研究室）
1月14日 10:00～12:00	同一セグメント内での VPN 構築の実験・実習（情報メディア研究室）
1月21日 10:00～12:00	同一セグメント内での VPN の相互通信実験（Windows XP,2000）
1月28日 10:00～12:00	離れた研究室間での VPN の相互通信実験（Windows と Linux）
1月29日・1月30日	情報メディア, 教育実践センター, 総合情報処理センター相互の VPN 通信実験

7. おわりに

インターネットの公衆回線でプライベートな専用回線を構築する技術である VPN を技術部の専門研修としてとりあげた. VPN の具体的な手法と VPN を実現する IPsec の基本概念は輪講形式で学習し, 実習は学内ネットワークの異なるセグメント間で IPsec による相互通信を行った. IPsec 通信の確認は, ネットワークに流れる通信データをパケットモニターでキャプチャして検証した.

今後 VPN の技術は, 研究室, 部局やキャンパス等の離れた端末機器へのアクセスに, セキュリティ対策の強化, 通信コストの削減並びに業務の効率化等が期待でき普及するものと思われる.

最後に, 本研修を遂行するにあたり, 日常的にご支援をいただいた総合情報処理センターの専任教員田中光也講師, 実習等で研究室を快く提供していただいた情報・メディア工学科浅田勝彦教授に深く感謝申し上げます.

参考文献

矢次弘志著：「IPsec による VPN 構築ガイド［基礎と実践］」, ㈱技術評論社, ２００３年発行
歌代和正監訳, 須田隆久訳：「VPN」, ㈱オライリー・ジャパン, ２００３年発行
小森哲郎：「ゼロからはじめる VPN」, ㈱アスキー, ２００３年発行
永井　建：「LAN ケーブルの作り方」, 福井大学総合情報処理センターニュース, Vol.17, No.2